(Modified) PATENT AND TRADEMARK OFFICE			ATTY DOCKET NO.	SERIAL NO.				
(-2	242895US2SRD	NEW A	EW APPLICATION		
	DE-E-	SEMOSE CITED BY AD	DU 10 44 F	APPLICANT				
LISTOF	KEFE	RENCES CITED BY AP	PLICANI	Hideo SHIMIZU, et al.				
				FILING DATE		GROUP		
				HEREWITH				
				U.S. PATENT DOCUMENTS				
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS			LING DATE PPROPRIATE
	4							
	AB							
	AC							
	AD							
	AE		<u> </u>			 		
	AF		<u> </u>		<u> </u>			
	AG							
	AH				 			
	Al				-			
	AJ		 					
	AK				 			
	AL		<u> -</u>					
		- · · · · · · · · · · · · · · · · · · ·	<u> </u>		ļ			
	AM				-			<u> </u>
	AN		<u> </u>	<u></u>		<u> </u>		
			FO	REIGN PATENT DOCUMENTS				
		DOCUMENT NUMBER	DATE	COUNTRY	TRANS YES		LATION NO	
CN	AO	2000-47833	02/18/00	Japan				×
CN	AP	2000-315201	11/14/00	Japan		<u> </u>	i i	×
CN	AQ	2000-322280	11/24/00	Japan				×
CN	AR	2002-23999	01/25/02	Japan			ĺ	×
	AS							
	AT		 					
	AU		<u> </u>					
	AV	· · · · · · · · · · · · · · · · · · ·					<u> </u>	
		OTHER RI	FERENCES (Including Author, Title, Date, Pertinen	t Pages, e	tc.)		
	OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, etc.) R. SCHROEPPEL, et al., "Fast Key Exchange with Elliptic Curve Systems", CRYPTO '95, LNCS 963, 1995, pgs. 43-56							
CN	AW							
CN	AX	A. J. MENEZES, et al.	, "Handbook o	f Applied Cryptography", CRC PRESS, 1	997, pgs.5	91-634		
	AY							
	AZ				☐ Add	itional Refe	erences	sheet(s) attached
Examiner /Chuong Ngo/					Date Considered 10/23/2006			0/23/2006
*Examiner: Ir conformance	nitial if r and no	eference is considered, ot considered. Include c	whether or no opy of this form	t citation is in conformance with MPEP 6 n with next communication to applicant.	09; Draw li	ne through	citation	if not in

				FILING DATE September 15, 2003			GROUP 2124					
			•									
				U.S. PATENT DOCUMENTS		<u> </u>						
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUB CLASS		LING DATE - PPROPRIATE				
	AA											
	AB											
	AC											
	AD											
	ΑE											
	AF											
<u></u>	AG											
	АН											
	Al			_								
<u>.</u>	AJ											
	AK											
	AL											
	AM											
•	AN											
			FC	REIGN PATENT DOCUMENTS								
		DOCUMENT NUMBER	DATE	COUNTRY		TRANSLATION YES NO		LATION NO				
	AO											
	AP											
	AQ	•										
	AR						Î					
	AS											
	AT											
	ΑU											
	ΑV											
		OTHER R	EFERENCES	Including Author, Title, Date, Pert	inent Pages, e	tc.)						
CN	AW	Hannes BRUNNER, et al., "On Computing Multiplicative Inverses in GF (2 ^m)", IEEE TRANSACTIONS ON COMPUTERS, vol. 42, no. 8, August 1993, pages 1010-1015										
	AX											
	AY											
	AZ						_					
						Additional References sheet(s) attache						
xaminer /Chuong Ngo/						Date Considered 10/23/2006						

.